Contactless Payment Systems: Credit Cards and NFC Phones

Peter Gutmann

University of Auckland

Contactless Payment Systems

Implemented as a standard credit-card payment mechanism running over RFID/NFC transport

- US: Magstripe card data dump in plaintext
- Non-US: EMV
  - Standard smart-card based payment mechanism, a.k.a. Chip and PIN

Completely standard, established mechanisms, but removing the need for a physical comms channel

Contactless Payment Systems (ctd)

Proprietary protocols for fare and stored-value cards, e.g. Mifare (1st-gen), T-Money (2nd-gen)

- Works in areas where EMV/credit cards aren't feasible
  - Microtransactions
  - Stored-value
  - …
- Not limited to the awkward plastic-card form factor

Mifare is completely broken from top to bottom

- T-Money status is unknown

Contactless Payment Systems (ctd)

NFC-enabled phones are much like contactless credit cards

- Emulate a standard contactless card

Since they have their own power, they can also initiate comms

- Act as NFC/RFID readers

Lots of competing standards and mechanisms

- Straightforward card-emulation will probably win out

Contactless Payment Systems (ctd)

Summary: Standard EMV protocol with the physical interface replaced by RFID/NFC

The End

Why Contactless?

A brief history of payment systems

- Barter
- Bullion coinage — gold, silver
- Fiat currency — paper notes
- Cheques
- Credit cards
- Smart-card credit cards
- Contactless smart-card credit cards

Why Contactless? (ctd)

The further removed you are from the physical expression of value, the more likely you are to part with it

- The more recent entries in the progression make it frighteningly easy to spend money

Banks ♥ Credit Cards

Credit card interest rates are 15-20% due to them being high-risk unsecured loans

- New Zealand has $5.6 billion owing on credit cards, of which $3.5 billion attracts interest

US has ~$800 billion in credit card debt

- See "Credit card statistics, industry facts, debt statistics" at `creditcards.com`

Banks ♥ Credit Cards (ctd)

Particularly problematic in the US, where credit card management is riddled with additional fee triggers and high-interest rate conditions

- Banks are allowed to raise any interest rate at any time by changing the account agreement
- Low promotional rates can be revoked after a single late payment
  - Half of all consumers pay late at least once a year
  - Younger (18-30) cardholders are far more likely to do this than older (60+) ones
- Most cards with penalty-rate agreements don't reset the rates when payments are made on time

Banks ♥ Credit Cards (ctd)

Even conscientious users who always settle on time are tripped up using a whole range of tricks

- Double-cycle billing
  - Base interest calculations on average balances from the previous two billing cycles
  - Hits people who pay off the minimum payment each month
- Banks preferentially pay off low-tier interest balances before high-tier ones
- Banks don't decline over-the-limit transactions but allow them and charge a huge penalty rate

See GAO report GAO-06-929, "Increased Complexity in Rates and Fees Heightens Need for More Effective Disclosures to Consumers"

Banks ♥ Credit Cards (ctd)

Entry barriers to credit card fraud are very low, and there's no incentive among banks/credit agencies to fix anything

- Bank recovers the money via a chargeback to the merchant
- Bank can also hit the merchant with chargeback fees
- If done right, the bank can actually *make money* from the fraud
  - Talk about a perverse incentive!

Fraud is cashflow-positive to card vendors

- It's income either way

Banks ♥ Contactless Credit Cards

Business plan for wallet-style functionality in smart phones

- Store keys in a hardware TPM
  - Just a hardwired smart card
- Charge for the use of the key slot
- Charge a percentage for each transaction
- Charge the user for having the wallet storage

In addition the merchants get charged at the other end for the transaction

Taken straight from dotcom-bubble la-la land, but that's how it's being pitched to stakeholders

Banks ♥ Contactless Credit Cards (ctd)

You have no idea where these things are ending up

> I often ask people if they have an RFID card and half the people emphatically say no I do not. And then they pull out the cards to prove it and … there has been an RFID in their wallet. This stuff is being deployed without people knowing it
> — Kristin Paget

How many people here have a contactless-payment device (card, phone, etc) with them?

Banks ♥ Contactless Credit Cards (ctd)

Do any of the cards in your wallet have something like this on them?

If they're present on a card then it's RFID-enabled

Banks ♥ Contactless Credit Cards (ctd)

Check *everything*, not just credit cards

- ZOMGWTF!
- Why does my *frequent flyer card* allow credit-card skimming?!!?

So What's the Problem?

Smart cards

- Need to explicitly establish a physical channel to the card
- Need to explicitly authorise a transaction via PIN entry

Contactless smart cards

- No need to establish a physical channel to the card
- No need to explicitly authorise a transaction

So What's the Problem? (ctd)

Contactless channel decouples the card/phone from the reader

- Security analysis of RFID passport risks explains it well

  The Department of State did not adequately consider how adding an RF transponder to the passport transformed it from an inert identification document to a remotely readable technological artifact

  — "A Case Study of the Security and Privacy Risks of the US e-Passport"

So What's the Problem? (ctd)

Use of this disconnected channel greatly eases fraud

Decades-old concept known as the Mafia fraud

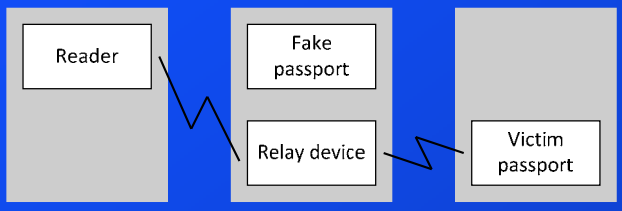
- Pay for pizza in New York
- Card is charged in Columbia for cocaine

Various other names, e.g. the chess grandmaster attack

- Play two chess grandmasters in different rooms off against each other

So What's the Problem? (ctd)

With ePassports (another common RFID technology) you actually need to spoof the passport to carry out the Mafia fraud



So What's the Problem? (ctd)

This might get noticed…

So What's the Problem? (ctd)

With contactless payments on the other hand, the most convenient attack device is also the payment device

Is this a relay attack or a genuine payment?

So What's the Problem? (ctd)

Mafia-fraud attack was demonstrated by a student in 2006 using homebrew gear

- Attack was on an ISO 14443 crypto card over a 1-foot (30cm) distance

  To demonstrate that it is not difficult to build the system locally to carry out the Mafia fraud attack on RFID
  — "RFID Insecurity for Entity Authentication"

Other attacks are also enabled through this decoupling

- Gerhard Hancke demonstrated a MITM attack on the Mifare card with on-the-fly modification of data using a reprogrammed commercial reader

So What's the Problem? (ctd)

Other groups have also done this using basic off-the-shelf gear

Source: www.ibnfc.org

So What's the Problem? (ctd)

Phone-based card skimming (without the payment portion) was demonstrated live at KiwiCon 2011

Enter the world's first mobile, PCI compliant credit card skimmer — "Mobile Apps and RFID — The Tale Of Two Techs"

So What's the Problem? (ctd)

These attacks are explicitly enabled by the use of the contactless interface

> It is, therefore, a bit surprising to meet an implementation that actually encourages rather than eliminates these attacks
> — "A Note on the Relay Attacks on e-passports: The Case of Czech e-passports"
>
> Our attack is only possible because the e-passports contain an RFID tag. If e-passports used a contact based smart card then such attacks would not be possible
> — "A Tracebility Attack against e-Passports"

What about EMV?

Cards talk to POS terminals that expect magstripe cards

- Readers output plaintext magstripe data, ignoring the EMV stuff
- Copy the result to a card and you're done

Skimming-only attack was first demonstrated by Pablos Holman on BoingBoing TV in 2008

> We got a reader off eBay for eight dollars
> — Pablos

What about EMV?

Full attack was demonstrated live by Kristin Paget at Shmoocon 2012, "Credit Card Fraud: The Contactless Generation"

- `http://www.shmoocon.org/2012/videos/CreditCardFraud.m4v`
- Watch this talk!

> The cardholder information that is used during a contactless payment transaction is of little to no use in creating fraudulent payment transactions
> — Smart Card Alliance

> It is unlikely that the details from the PayPass chip could be read and then copied onto the magnetic stripe of a counterfeit card
> — MasterCard

What about EMV? (ctd)

The people pushing the technology know about this issue, but don't care

> The premise that this is a new threat is absolutely false and isn't supported by [Paget's] demonstration
> — Randy Vanderhoof, Smart Card Alliance

> The truth is that consumers should be embracing this technology because it's making them safer
> — Randy Vanderhoof, Smart Card Alliance

What about EMV? (ctd)

Implementations in devices like phones are better than the ones in cards

Android only allows NFC activity when the screen is powered up and the device is unlocked

- Android logging is hit-and-miss
  - Records that an access took place, but not the UID that performed it
  - NFC activity logs are transient
  - Wiped on reboot/restart

What about EMV? (ctd)

Blackberry allows NFC activity even when the device is locked and/or powered off

- Like RIM, this problem will probably fade away

No-one's really sure what Apple's up to

What about no-EMV?

US card vendors took the easy way out in making their contactless cards compatible with mag stripe cards

- Send ISO 7813 track 1+2 data to the reader as if it was a mag stripe read

  The full cardholder name and card expiration date were present in cleartext in all transactions

  — "Vulnerabilities in First-generation RFID-enabled Credit Cards"

  – "It's the same info that's in the mag stripe, what's the problem?"

What about no-EMV? (ctd)

As a result, US contactless credit cards can be skimmed remotely without having to speak EMV

- Through the mailer when it's delivered
- From the wallet in your pocket

  Mr. Heydt-Benjamin was able to purchase electronic equipment online using a number skimmed from a card he ordered for himself and which was sealed in an envelope

  — New York Times

What about no-EMV? (ctd)

Initial eavesdropping tests were done with an antenna connected to an oscilloscope

- Skimming was done with a homebrew reader/emulator

  All of the RFID cards responded to our emulator exactly as they respond to a commercial RFID credit card reader

  — "Vulnerabilities in First-generation RFID-enabled Credit Cards"

Cards used a variety of homebrew protocols that dumped tracks 1+2 in various formats

What about no-EMV? (ctd)

Tag emulators are freely available

- Open-source circuit details, PCB layout, Gerber files
- Can also buy pre-built

What about no-EMV? (ctd)

Jonathan Westhues' proxmark3, the Rolls Royce of RFID tools

Source: cq.cx/proxmark3.pl

- DSP-based LF/HF universal RFID device with FPGA assist

What about no-EMV? (ctd)

Implemented as software-defined radio (SDR) so it goes beyond the capabilities of any standard reader to allow things like side-channel analysis/attack

- Sample config can read a TI 'glass transponder', read and clone a VeriChip, read and clone a Motorola FlexPass, read an ISO15693 tag, ...

Available in open-source form (Verilog, schematics, Gerbers, software, docs)

What about no-EMV? (ctd)

Mythbusters were planning to devote an episode to RFID credit-card security flaws

> Linda and Tory get on the phone and Texas Instruments [RFID manufacturers] comes on along with chief legal counsel for American Express, Visa, Discover, and everybody else. And I get chills just as I describe it… They […] absolutely made it really clear to Discovery that they were not going to air this episode talking about how hackable this stuff was, and Discovery backed way down. Tory still gets a little white when he describes that phone conversation
>
> — Adam Savage, Mythbusters

- Details of the story were later amended (only one legal counsel present, rest were managers; company was Mythbusters' own 'Beyond Productions' and not Discovery)

What about no-EMV? (ctd)

Channel 3 News, Memphis had an investigator walk down the street "looking for RFID chips to read, and credit card information to steal"

> Even people who thought there was no way we could pick their pocket electronically without laying a hand on them soon learned they were wrong. "You have a SunTrust card in there", Augustinowicz explained to a second "victim". "And that's your account number and expiration date"
>
> — "Electronic Pickpocketing"

Issuers insist that this isn't a security problem

> Would you be comfortable wearing your name, your credit card number, and your card expiration date on your T-shirt?
>
> — New York Times

What about no-EMV? (ctd)

These cards appear to have no actual security

> American Express said its cards incorporate "128-bit encryption" and J. P. Morgan Chase said its cards use "the highest level of encryption allowed by the U.S. government". But tests on 20 cards from Visa, MasterCard and American Express found the cardholder's name and other data was being transmitted without encryption and in plain text
>
> — New York Times

> Personally-identifying information (PII) is broadcast in cleartext by every RFID-enabled credit card we have examined
>
> — "Vulnerabilities in First-generation RFID-enabled Credit Cards"

What about no-EMV? (ctd)

The same problems have been found in a range of other RFID tokens

- German airport security-zone access cards could be easily cloned

  > We were shocked to discover that there were no security measures in place to prevent cloning
  >
  > — Der Spiegel (translated)

- Cloning an access card could be done while standing next to an airport employee on an escalator

  > Upgrading 15,000 access cards and 500 readers was ruled out due to cost issues
  >
  > — Der Spiegel (translated)

What about no-EMV? (ctd)

Vendors claiming security measures that don't actually exist is quite common with RFID (and, in general, embedded devices)

> Although RFID-enabled credit cards are widely reported to use sophisticated cryptography […] all the cards are susceptible to live relay attacks, all the cards are susceptible to disclosure of personal information, and all the cards are susceptible to various types of replay attacks
>
> — "Vulnerabilities in First-generation RFID-enabled Credit Cards"

What about no-EMV? (ctd)

You have no way of knowing what capabilities lurk inside these devices

California FasTrak road toll passes were supposed to be read-only

- Nate Lawson found that they were writeable

> FasTrak is probably not aware of this
>
> — Nate Lawson

What about no-EMV? (ctd)

You also have no idea what capabilities don't lurk inside these devices

> In the past, authorities have insisted that the FasTrak system uses encryption to secure data [...] But when Lawson opened up a transponder, he found that there was no security protecting these IDs
>
> — MIT Technology Review

- c.f. the missing encryption in contactless credit cards

What about no-EMV? (ctd)

Even industry insiders were unaware of what their own technology did

> That sentence [pointing out problems] makes us think this guy Lawson is an amateur. The only "research" needed to establish whether anything could be planted on the FasTrak transponder is a visit to the website of the manufacturer, Sirit. This makes clear what everyone in the toll business knows, namely that the FasTrak transponder is a read-only device which cannot have anything written to it at all
>
> — TOLLROADSnews commentary

- "That sentence makes us think this guy Columbus is an amateur. Everyone knows that if you sail too far into the Atlantic, you fall off the edge of the world"

What about no-EMV? (ctd)

> If Lawson has not even established that FasTrak transponders are a read-only device rather than read-write, then he's totally unqualified to be talking about potential misuse
> — TOLLROADSnews commentary

- This is scary: Industry experts are clueless about what their own products do
  - Insert joke about "a used car salesman knows when he's lying"

Protection Mechanisms that Aren't

CVV (3-digit number on back of card) is changed for each read

- You only get one valid card number and CVV per read
- To defeat this, read the card multiple times
  - Awkward with a mag stripe card, easy with a contactless card

Mass-harvest cards to defeat fraud checking

- Perform one transaction on each harvested card

Magstripe fraud = 1 person, 50 charges on the card

- RFID card fraud = 50 people, 1 charge on the card

Protection Mechanisms that Aren't (ctd)

Fraud checking by banks is very simplistic

- Example: 3 transactions against the same card from the same terminal

Can fingerprint what each bank does in terms of fraud checking

- Skim a bunch of cards
- Run transactions until you get a "declined" response

Don't do that any more for future skimmed cards

Shielding

RFID devices can be read through shielding

- Typical passport shielding bags provide about 7-8dB of attenuation
  - Some vendors claim 80dB or more of attenuation
  - They're confusing a cloth bag using metallised threads with a Faraday cage
  - Faraday cages have to be grounded

Shielding bag reduces the signal strength but doesn't block it

- Kristin Paget tested a range of these and found a variation of 50dB (factor of 100,000) between the best and the worst shields

Shielding (ctd)

Effectiveness also depends on

- The frequency (125kHz vs. 13.56 MHz vs. 900 MHz)
- Whether the shield is brand-new or crumpled from use
  - Some got better, some got worse with age and use

125kHz was particularly bad

- Only one single product stopped an unmodified reader from reading an unmodified tag

Shielding (ctd)

13.56MHz is right next to the 20m (14Mhz) amateur radio band

- Boost the range using off-the-shelf amplifier and antenna technology

Maximum practical range is probably about 10 metres

- 5W power output is OK, 20W kills cards

Shielding (ctd)

Some countries have (belatedly) proposed using foil inserts in passport booklets as a protection mechanism

- Could be applied to wallets holding credit cards as well

Riddle: What do you get when you place a metallic reflector behind an active element?

Shielding (ctd)

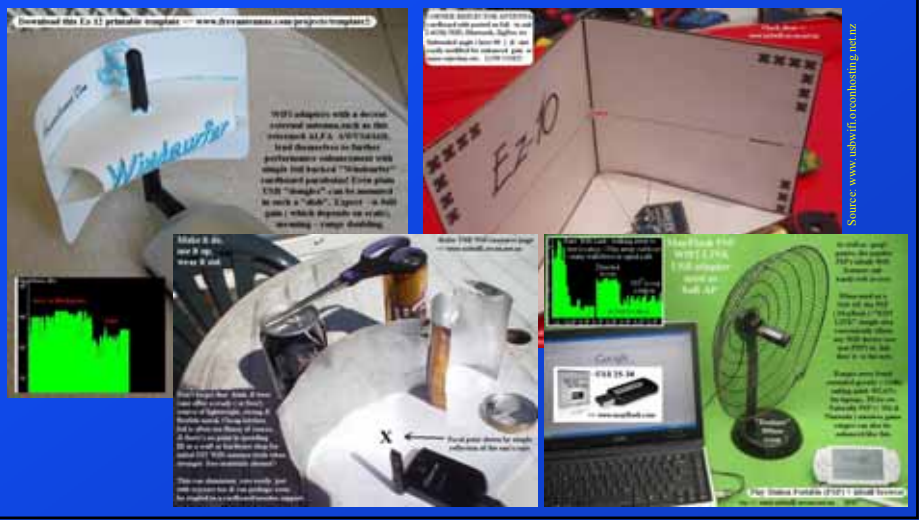
Riddle: What do you get when you place a metallic reflector (the shield) behind an active element (the tag)?

Answer: You get a *dish antenna*

- Stuff a few banknotes, receipts, and cards in a wallet with an insert and things can get worse than before

Shielding (ctd)

This is a standard trick used with cheap wireless gear to extend the range



Remote Reading

Security by executive fiat

> The proximity chip technology utilized in the electronic passport is designed to be read with chip readers at ports of entry only when the document is placed within inches of such readers
>
> — US Department of State, Public Notice 5208

Attack demonstration at Cards Asia conference in Singapore ("ePassport Privacy Attack", Harko Robroch)

- Intercepted passport ↔ reader communications from 5m away
  - Eavesdropping on terminal was possible from 25m away

Remote Reading (ctd)

Attack demonstration at BlackHat 2005 conference ("Long Range RFID and its Security Implications" Kevin Mahaffey)

- Read RFID tags from 50 feet away via a high-gain antenna
- Even longer distances are possible, but the demo was limited by the room size

Gerhard Hancke intercepted tag communication over 4m distance using standard off-the-shelf gear (Philips MF RC530 reader combined with Dynamic Sciences R-1250 receiver)

Another researcher read a tag from 25m away using a 4W reader

Remote Reading (ctd)

It's a good thing the long-range readers that were used for these demos don't know that they're not permitted to do this

> The ISO 14443 RFID specification permits chips to be read when the electronic passport is placed within approximately ten centimeters of the reader
> — US Department of State, Public Notice 5208

- Translation: The cheapest possible reader build from the cheapest possible parts should still more or less work over a 10cm range

Remote Reading (ctd)

Contactless payment cards aren't allowed to do this either

> Unlike RFID, which can operate at ranges up to 25 feet, contactless payment devices are designed with RF enabled technology that operates at very short ranges, less than 2-4 inches
>
> — Discover

> To authorize a payment, you must wave your Visa Micro Tag directly within 1-2 inches of a secure reader at an authorized merchant, and it must be properly oriented
>
> — Visa

Remote Reading (ctd)

What's the maximum effective range for assorted widely-used wireless technologies?

- 802.11 / WiFi?
- Bluetooth?
- EPC (Gen2) product tags?
- 13.56MHz tags?

Remote Reading (ctd)

802.11 / WiFi

- 300km (Monte Amiata, Tuscany to Monte Limbara, Sardinia)
  - Limited by the curvature of the earth
- CISAR, Italy, 2007

Bluetooth

- 1.8km
- trifinite team, 2004

Remote Reading (ctd)

EPC tags

- 217 feet / 70 metres
  - Range was limited by clutter from the test environment
- Kristin Paget, 2010

13.56Mhz tags

- Probably 10-20 metres

Implementation Vulnerabilities

Several attacks on wireless device stacks have already been demonstrated

- Example: Trifinite's BlueSmack attack on Toshiba's Bluetooth stack caused an instant BSOD on the host

Codenomicon's Bluetooth testing found even worse problems

> Most of the Bluetooth-enabled devices simply crashed when tested with any level of robustness testing. Sometimes the result from the testing was that the device ended up totally corrupt, requiring re-programming of its flash memory to become operable
> — "Wireless Security: Past, Present, and Future"

Implementation Vulnerabilities (ctd)

Other devices were no better

> All the [802.11] access points failed with some of the protocol tests, but more alarmingly there were access points that failed with almost everything that was run against them
> — "Wireless Security: Past, Present, and Future"

Overall result of wireless device testing was abysmal

> Testing found problems in 90 percent of the devices tested
> — "Wireless Security: Past, Present, and Future"

This was straight fuzzing, not even a targeted, device-specific attack!

Implementation Vulnerabilities (ctd)

IFDs/ICCs make SCADA systems look good in comparison

- Writing an IFD/ICC driver isn't so much implementing a spec as finding (by trial and error) the appropriate silly-walk to induce a given device and firmware combination to provide the intended result

  Conformance to this standard does not assure that a particular implementation is secure
  — FIPS PUB 201-1

Implementation Vulnerabilities (ctd)

Readers/devices will…

Hang (requiring a soft reset)

Lock up (requring a power cycle)

Return invalid data lengths (too much/too little)

- The ICAO has already run into some of these bugs during interop testing

  We have found that some cards expect 4-byte and some 5-byte APDU when Le = 00
  — ICAO 9303 supplement 2005-4

… continues …

Implementation Vulnerabilities (ctd)

… *continued* …

Return invalid data (tags, field lengths, element counts, field entries, ...)

> Three different implementations were found at read binary of Odd_INS Byte when reading data greater than 32k byte
>
> 1) The Le byte contains V only.
> 2) The Le byte contains TL and V.
> 3) The Le byte contains extended TL and V
>
> — ICAO 9303 supplement 2005-4

- Extensive bug lists in amendments to ICAO 9303 provide a roadmap of attack vectors to try

… *continues* …

Implementation Vulnerabilities (ctd)

… *continued* …

Require invalid data (reject correctly-formatted data)

- This one is especially entertaining to figure out

React to commands in unexpected/undefined ways

> From our Singapore InterFest experience, we know some card vendors expect Le = 28 and some expect Le = 00 or will only respond correctly if Le = 00
>
> — ICAO 9303 supplement 2005-4

- This includes doing things that shouldn't be permitted

… *continues* …

Implementation Vulnerabilities (ctd)

… continued …

Implement undocumented commands or command extensions

- This is very common
- Some are bugs, some are just vendor-specific supplementary functionality
  - ISO 7816-4 defines different classes of command, CLA '0x' = standard, CLA '8x' / '9x' = vendor-specific
  - Vendors implement the bare minimum of CLA '0x'
  - As much functionality as possible is implemented in CLA '8x' / '9x' to prevent interoperability

… continues …

Implementation Vulnerabilities (ctd)

Parsers for card data are notoriously brittle

- It's easy to crash readers (IFDs) simply by sending malformed data

Use the tag contents to attack the reader

- Modify the tag data to exploit flaws in readers

Lukas Grunwald modified the ePassport's JPEG2000 image to exploit buffer overflows in passport readers

> They could be vulnerable to a code-injection exploit that might reprogram a reader to approve expired or forged passports
> — Wired

Will it be Exploited?

The current state of card compromise

We sell all you need to hack, shop & cashout.

Cvv2 = UK, EU, ASIA,CA and AU

VBV (Verified By Visa) = UK and US only

VISA CLASSIC|MASTERCARD $5 <> $3 per 30

VISA PLATINUM|BUSNESS $10 <> $7 per 30

VISA SIGNATURE $20 (when available)

Bank Details e.g Accnt #, Routine and so on… and Background details e.g SSN, DL, MMN, DOB and PIN

Contactless card skimming just isn't enough of a target

- Far easier ways to get at card data

Will it be Exploited? (ctd)

However: Story parallels UK banks' attitude to ATM security in the 1990s

- Card skimming (white-card fraud) was easy for anyone in the know
- Demonstrated live on TV by security researchers
- Banks threw lawyers at anyone who claimed there was a problem
  - Led to some appalling miscarriages of justice
  - See Ross Anderson's publications for more on this
- Late-90s court decisions forced banks to fix things
- Outcome was Chip and PIN

Summary

This stuff is quietly being rolled out everywhere

Enables a whole range of attacks that were never possible with standard cards

- No protection against skimming attacks
- No protection against Mafia fraud

Best analogy for security

- You're handing your credit card to anyone in the vicinity to do with what they want